

de Mars S, O'Callaghan P.

[Privacy and Search Engines: Forgetting or Contextualizing?](#)

Journal of Law and Society 2016, 43(2), 257-284.

Copyright:

This is the peer reviewed version of the following article, which has been published in final form at <http://dx.doi.org/10.1111/j.1467-6478.2016.00751.x>. This article may be used for non-commercial purposes in accordance with [Wiley Terms and Conditions for Self-Archiving](#).

Date deposited:

26/01/2016

Embargo release date:

10 February 2017

Privacy and Search Engines: Forgetting or Contextualizing?

SYLVIA DE MARS* AND PATRICK O'CALLAGHAN**

This paper considers the much-criticised 'right to be forgotten' in the context of the European Court of Justice's judgment in the Google Spain case. It defends the 'right to be forgotten' as a metaphor that can provide us with a better understanding of the particular privacy concerns of the search-engine age and their interaction with the freedom to access information. In unpacking this metaphor and putting it to use, the paper draws on Erving Goffman's idea of 'information games' and Helen Nissenbaum's theory of 'contextual integrity'. While supporting the principles that underpin the Google Spain judgment, the article rejects the Court's binary approach of 'forgetting' versus 'remembering' personal information. Instead, it argues that the EU legislator should introduce more nuanced means of addressing modern privacy concerns. By establishing two remedies—'delisting' or 'reordering', depending on the nature of the information in question—online information flows can be adjusted so as to preserve both the right to privacy and the freedom to access information in more contextually appropriate ways.

INTRODUCTION

Rarely has a decision of the Court of Justice of the European Union (ECJ) triggered the sort of media frenzy that followed the case of *Google Spain* and its purported establishment of a 'right to be forgotten' on the internet.¹ Charges that the decision would lead to censorship of speech featured prominently in public discourse. Reactions of this sort are in many ways understandable. As Bernal has argued, the terminology causes or 'provokes emotional and instinctive reactions.'² Our instincts tell us that the words 'law' and 'forgetting' should not mix. Requiring us to forget or erase details from public record is the sort of activity we might ordinarily associate with totalitarian regimes. Here, as Hitchens puts it, ideology seeks to 'begin the human story over again', becoming a 'cult of the now'.³ Consider in this light the Khmer Rouge's ruthless attempts to bring about 'year zero'.⁴ Thoughts such as these generate, as Ricoeur rightly emphasises, 'uneasiness' in us.⁵

However, the Court's decision in *Google Spain* is not as radical as it first appears.⁶ Rather, it is more nuanced, focussing on the special status of search engines as a primary means

* Newcastle Law School, Newcastle University, 21-24 Windsor Terrace, Newcastle upon Tyne, NE1 7RU
sylvia.de-mars@ncl.ac.uk

** School of Law, Áras na Laoi, University College Cork, Cork, Ireland
patrick.ocallaghan@ucc.ie

The authors thank Steve Hedley and the anonymous reviewers for their critical and thoughtful comments.

¹ Case C-131/12 *Google Spain SL v AEPD* [2014] ECLI:EU:C:2014:317; see, for instance, A. Travis and C. Arthur, 'EU court backs "right to be forgotten": Google must amend results on request' *Guardian*, 13 May 2014 <<http://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results>>.

² P. Bernal, 'A Right to Delete' (2011) 2(2) *European Journal of Law and Technology* <<http://ejlt.org/article/view/75/144>>.

³ C. Hitchens, *Arguably* (2011) 162.

⁴ See further F. Ponchaud, *Cambodia: Year Zero* (1978).

⁵ P. Ricoeur, *Memory, History, Forgetting* (2004) 501.

⁶ See also O. Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD* and *Mario Costeja González*' (2015) 78 *Modern Law Rev.* 522, at 528; A. Roughton, 'Google and the "right to be forgotten" –

of accessing information in the digital age. Understood in this way, the Court's position is not simply that individuals should have a licence to erase information from the internet at will. Rather, the decision seeks to ensure that when interests in forgetting/being forgotten are at stake, *certain* types of information should not be so easily and readily accessible. This does not mean that the information cannot be accessed in other ways; rather, that in the absence of a public interest, such information should not be instantly available by typing a person's name into a search engine.⁷

In this paper, we aim to explain and justify the principles that lie behind the Court's decision in *Google Spain*. After detailing the judgment, we argue that the 'right to be forgotten' is a useful metaphor as it helps us 'make sense' of our experiences of technological development and the associated social change. Indeed, there are two reasons in particular why the 'right' is so helpful. First, the distinct privacy challenges of the 21st century are revealed once we contrast the 'right' with another metaphor: digital technology's capacity for 'perfect memory'. Second, because the terminology of a 'right to be forgotten' is instinctively contentious, it forces us to consider the implications of data erasure for the freedom to access information.

Building on the work of Erving Goffman and Helen Nissenbaum, amongst others, we argue that sometimes it is better to obtain limited or reordered results from an internet search engine as long as this preserves 'contextual integrity'. Though we identify problems with a blunt-force application of these ideas about 'forgetting' and 'being forgotten', we argue that properly developed remedies that strive for 'contextual integrity' have the potential to be important tools in protecting both the rights to privacy and information on the internet.

GOOGLE SPAIN V AEPD

Google Spain is the culmination of five years of effort by Mr. Mario Costeja González to have information about himself removed from Google's search results. His journey commenced in 2009, when he discovered that upon searching for his name through Google, Google produced links to two Spanish newspaper announcements from 1998. These announcements concerned a real-estate auction of property owned by Mr. Costeja, prompted by his social security debts. In short, anyone searching for Mr. Costeja's name immediately found these twelve year old notices about his very much historical debts.⁸

Mr. Costeja's complaint to the Spanish Data Protection Authority (DPA), the AEPD, advanced two separate requests: removal of the original notices from the newspaper's archive, or alternatively, removal of the links to these notices from Google's search results for his name.⁹ What this suggests is that Mr. Costeja was most concerned about the fact that this information was easily and instantly available whenever anybody put his name into the search engine; not necessarily that it was available in a newspaper archive, where it was unlikely to be found by any internet user not specifically looking for it.¹⁰

In July 2010, the AEPD upheld Mr. Costeja's claim against Google, and consequently called on Google to withdraw the data from their index and render future access to these links

setting the record straight' (2014) 14(8) *Privacy & Data Protection* 6; J. Jones, 'Control-alter-delete: the "right to be forgotten"' (2014) 36(9) *European Intellectual Property Rev.* 595.

⁷ See P. Korenhof et al, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data' in *Reforming European Data Protection Law*, in eds. S Gutwirth et al (2015) 183.

⁸ Opinion of Advocate-General Jääskinen in Case C-131/12 *Google Spain SL v AEPD* [2014] ECLI:EU:C:2013:424, paras 18-19; *Google Spain*, op. cit., n 1, para 14.

⁹ AG Opinion in *Google Spain*, id., para 21; *Google Spain*, op. cit., n 1, para 15.

¹⁰ 'Ease of access' is what worries internet users with privacy concerns the most; see A.H. Stuart, 'Google Search Results: Buried if Not Forgotten' (2014) 15 *North Carolina J. of Law and Technology* 463, at 467.

to the newspaper announcements impossible.¹¹ Google appealed the AEPD's decision before the *Audienca Nacional*, which referred questions to the ECJ on the territorial scope of the EU's Data Protection Directive, the nature of Google's search engine's activities, and finally, if the Directive establishes a 'right to be forgotten' for persons in Mr. Costeja's position.¹²

The Court's ruling on all three of these questions has been discussed in detail at this time.¹³ For our purposes, the most interesting aspect of the judgment is its particular focus on the role that search engines play in our ability to access information and how they impact on our right to privacy. The Court highlighted that search engines have a far more extensive effect on data subjects' right to privacy than many publishers (such as newspaper archives), on account of their ability to disseminate information instantaneously and world-wide. The Court also found that this dissemination of personal data is not a process that Google only *permits*, but rather one it *controls*: consequently, it found that Google bears responsibility for ensuring that when it builds search result pages, it satisfies the requirements to protect personal data and private life set out in the Directive.¹⁴ The Court thus concluded that Google *is* responsible for removing links from its search engine where Articles 12(b) (establishing the right to erase, block, or rectify information, particularly where it is incomplete or inaccurate) or 14(a) (enabling data subjects to 'object at any time, on compelling legitimate grounds relating to [their] particular situation[s], to the processing of data relating to [them]....') of the Directive apply.¹⁵

Next, in considering if the Directive establishes a 'right to be forgotten', the Court found that the right to have data erased, blocked or rectified under Article 12(b) exists for data subjects whenever any of the conditions of Article 6 are not met.¹⁶ Article 6's obligations prohibit inaccurate and incomplete data, but they also cover data that is inadequate, irrelevant, disproportionate, not kept up to date, or kept for longer than is necessary.¹⁷ When a data subject files a request under Article 12(b) because data provided by a search engine's index is no longer 'up to date' or kept for longer than is necessary, as Mr. Costeja did in *Google Spain*, the Court found that Article 12(b) read in conjunction with Article 6 obliges a search engine to erase these links.¹⁸

The Court acknowledged that the referred questions involve a weighing of competing fundamental rights: these are the rights of data protection (Article 8 CFR) and respect for private life (Article 7 CFR) on the one hand, and the rights to freedom of expression and information (Article 11 CFR) and the freedom to conduct business (Article 16).¹⁹ However, it found that in cases of this nature, Article 7 and 8 rights will generally outweigh Article 11 rights. Its only caveat was that '[the nature of the balancing of the rights] may ... depend ... on the nature of the information in question and its sensitivity for the data subject's private life

¹¹ *Google Spain*, op. cit., n 1, para 17.

¹² *id.*, paras 18-20.

¹³ See Lynskey, op. cit., n 6; H. Hijmans, 'Right to Have Links Removed: Evidence of Effective Data Protection' (2014) 21 *Maastricht J. of European and Comparative Law* 555; D. Lindsay, 'The "Right to be Forgotten" by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling' (2014) 6 *J. of Media Law* 159; S. Stokes, 'A decision to quickly forget: Google Spain and Google on the right to be forgotten' (2014) 25 *Entertainment Law Rev.* 233; E. Kelsey, '*Google Spain SL and Google Inc v AEPD and Mario Costeja González*: protection of personal data, freedom of information and the "right to be forgotten"' (2014) 4 *European Human Rights Law Rev.* 395; G. Sartor, 'Search Engines as Controllers: Inconvenient Implications of a Questionable Classification' (2014) 21 *Maastricht J. of European and Comparative Law* 564.

¹⁴ *Google Spain*, op. cit., n 1, paras 35, 38, 80, 87.

¹⁵ *id.*, para 88.

¹⁶ *id.*, paras 72, 94.

¹⁷ *id.*, para 72.

¹⁸ *id.*, para 99.

¹⁹ *id.*, para 97.

and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.’²⁰

The Court concluded in *Google Spain* that as the information in question was 12 years old, no longer relevant, and as Mr. Costeja is not a public figure, the Directive enables Mr. Costeja to request that Google no longer link to it.²¹ However, while the referring court asked explicitly if Articles 12(b) and 14(a) amount to a ‘right to be forgotten’, the Court did not use those words at any point, finding only that Articles 12(b) and 14(a) of the Directive allow data subjects to contact a search engine and request it to edit or erase search engine results that are inaccurate, incomplete, outdated, or no longer relevant.

The Court thus did not create a general ‘right to be forgotten’; rather, it read existing EU legislation as containing the right to have certain types of information removed from search engine results. Controversy has stemmed from the attachment of the ‘right to be forgotten’ label to a judgment that was, in reality, more reserved.²² The Court focused on the specific function of the search engine on the modern internet and how it impacts the privacy of internet users. The Court concluded that search engines must have distinct, separate responsibilities from *other* data controllers on the internet. Far from being a radical new idea, the Court’s position, as we will argue next, is rooted in older and more familiar accounts of privacy and its interaction with competing rights.

THE CONTENT OF A ‘RIGHT TO BE FORGOTTEN’

1. The ‘Right to be Forgotten’ as a Metaphor

While the idea of a ‘right to be forgotten’ features in the doctrine and legal scholarship of several civil law legal systems in Europe,²³ it is only in recent years that the term has gained prominence at the EU level. In 2012, the European Commission published a proposal for a new Data Protection Regulation which, in Article 17, extended the ability for data subjects to object to data processing under EU law. In the original proposal, Article 17 was titled the ‘right to be forgotten and to erasure’.²⁴ However, few commentators thought that the terminology was suitable. Koops, for example, thought that using the label, a ‘right to be forgotten’, was an ‘error of judgement’. He went on:

‘The term “right to be forgotten” has been floated as an appealing ideal for doing something about the persistence of embarrassing data on the Internet, but it is pretty obviously a misnomer; not only is it very difficult to have all copies of data removed from the Internet, but removing content from the Internet also cannot be equated to people actually forgetting what they have already read.’²⁵

Similar concerns led the UK DPA, the Information Commissioner’s Office, to conclude that the label might generate unrealistic expectations. More specifically, the ICO was concerned that individuals might become ‘disillusioned’ if it emerged that the right was ‘limited in

²⁰ *id.*, para 81.

²¹ *id.*, para 99.

²² See, similarly, Lynskey, *op. cit.*, n 6, p. 528.

²³ See G. Brüggemeier et al. (ed.) *Personality Rights in European Tort Law* (2010) case 3.

²⁴ European Commission, *Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (2012) COM(2012)11 final.

²⁵ B.J. Koops, ‘The Trouble with European Data Protection Law’ (2014) 4 *International Data Privacy Law* 250, at 258-259.

practice’.²⁶ Indeed, perhaps for reasons of this sort, EU-level negotiations on the Data Protection Regulation have re-branded Article 17 to the ‘Right to erasure (“right to be forgotten”)’.²⁷

Whatever the limitations of using the term in the text of legislation, we argue that ‘the right to be forgotten’ is a helpful metaphor in attempting to better understand the complexities of the interaction between privacy and the freedom to access information in the digital age.²⁸ Markou, in an extensive critique of the term, acknowledges that the term itself may be a metaphor, and concedes that metaphors ‘[can help translate] new technological phenomena into legal issues (or rules)’.²⁹ Even so, she appears unconvinced that the ‘right to be forgotten’ is the right metaphor to use in this context. On her account:

‘whereas metaphors are, in the legal field, used to render difficult-to-grasp phenomena more understandable, the choice of the “forgotten” label strikingly seems to have involved the opposite. Indeed, what was at stake is something as concrete and understandable as “data erasure”, which has been described by reference to “forgetting”, a complicated and difficult-to-grasp psychological process!’³⁰

However, in our view, despite (or perhaps even because of) the fact that forgetting is a ‘complicated and difficult-to-grasp psychological process’, the terminology of a ‘right to be forgotten’ is extremely helpful in explaining why the tool of data erasure is needed in the first place.

It is instructive here to consider the etymology of ‘metaphor’. ‘Metaphor’ comes from the Greek *meta* (across) and *pherein* (carry).³¹ ‘The essence of metaphor’, as Lakoff and Johnson explain in their classic account, ‘is understanding and experiencing one kind of thing in terms of another.’³² The metaphor *carries* a meaning from one context *across* to another, and thus the right metaphor for a given situation helps us to ‘make sense’ of our experiences (thereby giving them a ‘coherent structure’).³³

Over the past few decades, we have witnessed rapid and extensive technological development (and ensuing social change). But we find it difficult to make sense of our experiences of this rapid change. This is because while cyberspace constantly expands, the capacity of the individual brain to process this information stays the same or barely changes.³⁴ Moreover, given how deeply embedded we are in this social change, it is difficult to achieve the necessary distance from it in order to measure the ‘emotional, psychological, and existential price’ we pay for our reliance on the Internet.³⁵

²⁶ Information Commissioner’s Office, *Initial Analysis of the European Commission’s Proposals for a Revised Data Protection Legislative Framework*, (27 February 2012) < <http://www.scl.org/site.aspx?i=xb997> > 13; see also M. Kuchewsky, ‘The Right to be Forgotten – the fog finally lifts’ (2012) 12 *Privacy & Data Protection* 10.

²⁷ European Council Presidency, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Confirmation of the final compromise with a vue [sic] to agreement (15321/15)* <<http://data.consilium.europa.eu/doc/document/ST-15321-2015-INIT/en/pdf>>

²⁸ For an influential account of the place of forgetting in the digital age, see V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (2009).

²⁹ C. Markou, ‘The “Right to be Forgotten”: Ten Reasons Why It Should Be Forgotten’ in Gutwirth et al. (eds.), *op. cit.*, n 7, p. 221.

³⁰ *id.*

³¹ I. McGilchrist, *The Master and his Emissary* (2009) 116.

³² G Lakoff and M Johnson, *Metaphors we live by* (1980) 5.

³³ *id.*, p. 139; on a metaphor’s potential to shape our thinking and behaviour, see also, Schön’s work on ‘generative metaphors’ and ‘framing’: D Schön, ‘Generative metaphor: A Perspective on Problem-Setting in Social Policy’ in *Metaphor and Thought*, ed. A Ortony (1993, 2nd edn).

³⁴ F. Berardi, *The Soul at Work: From Alienation to Autonomy* (2009) 100-101.

³⁵ *id.*, p. 90.

Understood in this way, while the metaphor of a ‘right to be forgotten’ may well prove to be too ‘woolly’ to feature in a legislative text,³⁶ we believe that it can help us conceptualise technological development and the associated social change in ways that ‘make sense’ of our experiences. Indeed, the metaphor is especially useful for two reasons, which we now turn to consider. Firstly, once we introduce the ‘right to be forgotten’ as an antithesis to another metaphor, digital technology’s capacity for ‘perfect memory’, our attention becomes drawn to the pertinent privacy concerns of today. Second, because the ‘right to be forgotten’ is at the same time instinctively contentious, it brings into sharp focus concerns about what data erasure might mean for the freedom to access information.

2. Forgetting and ‘Perfect Memory’: The Dual Nature of a ‘Right to be Forgotten’

The first reason why the metaphor of the ‘right to be forgotten’ is helpful is because it brings to our attention the particular privacy concerns of the 21st century. These concerns are revealed once we contrast the ‘right to be forgotten’ with another commonly-used metaphor: digital technology’s capacity for ‘perfect memory’.

Today’s ‘technological landscape’, as Nissenbaum explains, provides capacities to monitor, track and retain personal information in ways we could not even imagine just a few years ago.³⁷ Technology allows us to aggregate and analyse this information, which we can then disseminate and publish, quickly and easily.³⁸ Once published, this information may prove difficult to delete.³⁹ It is against this backdrop that scholars have written about the capacity for permanent data retention, or what Bellia calls the ‘architecture of perfect memory’.⁴⁰ While the internet does not currently retain every single piece of information forever,⁴¹ the metaphor of ‘perfect memory’ helps us to ‘make sense’ of the implications of technological development. In doing so, scholars have sought to investigate the implications of ‘perfect memory’ both for individual well-being and society as a whole.⁴² They argue that we risk suffering from ‘excessive remembering’ in our connected lives.⁴³ Mayer-Schönberger, for instance, has written of the ‘huge digital information treasure’ from which we can retrieve information in an instant. On his account, advances in technology have ‘facilitated a culture of creation, bricolage, and sharing in which we have abandoned traditional forms of information control.’⁴⁴ The result is that we have ‘little incentive to forget’.⁴⁵

While the privacy challenges of today appear different to those of the past, we argue that the idea of a ‘right to be forgotten’ is rooted in older conceptions of privacy.⁴⁶ Privacy has

³⁶ On ‘woolly’ concepts in law see D.L. Zimmerman, ‘False Light Invasion of Privacy: The Light that Failed’ (1989) 64 *New York University Law Rev.* 364, at 369.

³⁷ H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2010) 21-66.

³⁸ *id.*

³⁹ See generally Mayer-Schönberger, *op. cit.*, n 28.

⁴⁰ P.L. Bellia, ‘The Memory Gap in Surveillance Law’ (2008) 75 *University of Chicago Law Rev.* 137.

⁴¹ Indeed, much digital information risks disappearing over time; see, for instance, H. Gladney, *Preserving Digital Information* (2007), Chapter 1.

⁴² See, in particular, M. Augé, *Oblivion* (M de Jager (tr), 2004); J.F. Blanchette and D.G. Johnson, ‘Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness’ (2002) 18 *The Information Society* 33; L.J. Bannon, ‘Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing’ (2006) 2 *CoDesign* 3; Mayer-Schönberger, *op. cit.*, n 28.

⁴³ See Bernal, *op. cit.*, n 2; on ‘too much remembering’ see Mayer-Schönberger, *id.*

⁴⁴ Mayer-Schönberger, *id.*

⁴⁵ *id.*

⁴⁶ See, for recent work on privacy as a value in the data protection context, A. Rouvroy and Y. Pouillet, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Gutwirth et al. (eds.), *op. cit.*, n 7; F Ferretti, ‘Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?’ (2014) 51 *Common Market Law Rev.* 843, at 849-851.

long been understood as being essential for human personhood and especially important for the safeguarding of basic interests in autonomy and dignity.⁴⁷ Those scholars who advocate control-based understandings of privacy emphasise the link between privacy and *autonomy*.⁴⁸ Fried, for example, writes that ‘privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.’⁴⁹ Common to control-based accounts is the idea that the individual should be able to take control of her private life and, in doing so, decide on its parameters. As for *dignity*, privacy scholars argue that the absence of privacy is degrading.⁵⁰ Drawing on Warren and Brandeis’ account of privacy as ‘inviolate personality’, Bloustein argues that this principle ‘defines man’s essence as a unique and self-determining being.’ He contends that ‘[t]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity.’⁵¹

We argue that both the control-based and dignitarian accounts of privacy underlie what has become known as the ‘right to be forgotten’.⁵² This ‘right’ has a dual nature, as revealed in the language used in several other European legal systems. Consider, for example, the German and French equivalents, the *Recht auf Vergessen* or the French *droit à l’oubli*. As well as the individual having an interest in being forgotten by others, these linguistic formulations also point to a latent side of the ‘right’: the individual’s *own* interests in forgetting things from her *own* past.⁵³ Though there is significant conceptual overlap between the two, we will now consider each interest in turn as we argue the former gives expression to a *control-based* account of privacy and the latter a *dignitarian* account.

(a) The interest in being forgotten by others

We mentioned above that control-based accounts of privacy emphasise the connection between privacy and autonomy. ‘Normative agency’, in this sense, is important because it feeds into identity-formation.⁵⁴ Personhood is based on our individual sense of identity or *ichbewusstsein*.⁵⁵ But the construction of identity is a social as well as a personal process. Jaspers understood personality as ‘that mode of being oneself which, in its very nature, cannot

⁴⁷ J.Q. Whitman, ‘The Two Western Cultures of Privacy: Dignity versus Liberty’ (2004) 113 *Yale Law J.* 1151.

⁴⁸ See, for example, C. Fried, ‘Privacy’ (1968) 77 *Yale Law J.* 475; AF Westin, *Privacy and Freedom* (1967).

⁴⁹ Fried, *id.*, p. 482.

⁵⁰ E. Bloustein, ‘Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser’ (1964) 39 *New York University Law Rev.* 962; S. Warren and R. Brandeis, ‘The Right to Privacy’ (1890) 4 *Harvard Law Rev.* 193.

⁵¹ Bloustein, *id.*, p. 1003.

⁵² In a thoughtful paper about the ‘right to be forgotten’, Andrade links it to the ‘right to identity’ rather than privacy. See N. de Andrade, ‘Oblivion: The Right to be Different...from Oneself: Reproposing the Right to be Forgotten’ (2012) 13 *Revista de Internet, Derecho y Política* 122. This approach perhaps makes more sense to civilian lawyers familiar with ‘personality rights’. While Andrade provides a compelling argument and we draw similar conclusions about the role of search engines in identity formation, we prefer to theorise the ‘right to be forgotten’ from a privacy perspective. This is for two reasons. First, we think there are distinct limits as to what the law can do in ensuring what Andrade calls the ‘correct projection’ of one’s identity, the nature of which, after all, is agent-relative and context-dependent. (On this point see further P. O’Callaghan, ‘False Privacy and Information Games’ (2013) 4 *J. of European Tort Law* 282). Second, in our view there must be some degree of truth (even if outdated) in the information in question if the agent has an interest in forgetting it. In this sense, we see the ‘right to be forgotten’, fundamentally, as a metaphor for privacy interests.

⁵³ On this distinction see further B.J. Koops, ‘Forgetting Footprints, Shunning Shadows: A Critical Analysis of the “Right to be Forgotten” in Big Data Practice’ (2011) 8 *Scripted* 229, at 231-232.

⁵⁴ Normative agency is our ‘capacity to choose and to pursue our conception of a worthwhile life’. See J. Griffin, *On Human Rights* (2008) 44.

⁵⁵ On *ichbewusstsein* see K. Jaspers, *Allgemeine Psychopathologie* (1913).

be alone; it is something related, must have something else apart from it: persons and nature.’⁵⁶ As social beings, not only do we seek to be accepted by others, we also use others as reference points in our personal development, in the same way that a child learns to play a game.⁵⁷

Notwithstanding the social aspect of identity-formation, normative agency surely requires that the individual exercises *some* degree of control over various information flows that contribute to shaping her identity. As Giddens puts it, she ought to have the ‘capacity to keep a particular narrative going’.⁵⁸ Ordinarily she does this through what Erving Goffman calls the ‘information game’. The ‘information game’ is a key feature of social interaction - ‘a potentially infinite cycle of concealment, discovery, false revelation, and rediscovery.’⁵⁹ In other words, social interaction is an inherently dynamic process within which the very identity of the individual is shaped. We routinely engage, Goffman argues, in ‘audience segregation’: we display different ‘fronts’ or we ‘play different parts’ depending on the individual or group with whom we are interacting.⁶⁰ In the digital environment, this explains why internet users often have multiple profiles when using the internet. These allow users to ‘present appropriate facets of themselves to others, understood as assuming a variety of roles in these respective contexts.’⁶¹ So, the individual may have one profile for her social media account, another for leaving comments on a newspaper’s website and another still for a dating website.⁶²

However, playing an ‘information game’ becomes more difficult online. This can be attributed, at least in part, to the blurring of traditional distinctions between the public and private spheres in the online context. For instance, when a user of a social networking site such as Twitter posts information online there is normally some level of awareness that the material is ‘online’ and thus ‘public’ but in many cases the target readership comprises of friends, colleagues, close relatives, and so on. But, without the proper privacy controls, this information will be picked up by Google and other search engines. An online search, then, has the potential to instantaneously create a collage of information about an individual’s personal life.⁶³ The playing of ‘information games’ is further complicated by the fact that search engine results publish not only information made available *by* that individual, but also information made available *about* that individual: the version of us presented by search engines consequently may differ radically from the version we ideally would present of ourselves in different situations. The individual can no longer exercise control over personal information in the way she would have done when engaging in an ‘information game’ in the pre-digital world.

If Google and similar search engines are indeed increasingly becoming our windows to the world,⁶⁴ then they have a profoundly important part to play in identity formation in the 21st century. Understood in this way, search engines are much more than simply repositories of information; rather they are active forces in identity formation. But, importantly, search engines make it more difficult for the individual to engage effectively in ‘information games’. This has profound implications for her ‘capacity to keep a particular narrative going’ and thus undermines individual autonomy. Furthermore, search engines prioritize certain types of sources in their rankings: information published in newspapers will generally be listed higher

⁵⁶ P.A. Schilpp, *The Philosophy of Karl Jaspers* (1957) 263.

⁵⁷ G.H. Mead, *Mind, Self, & Society* (1934).

⁵⁸ A. Giddens, *Modernity and Self-Identity* (1991) 54.

⁵⁹ E. Goffman, *The Presentation of Self in Everyday Life* (1959) 20.

⁶⁰ *id.*, p. 57.

⁶¹ Nissenbaum, *op. cit.*, n 37, p. 229.

⁶² See, similarly, J. Powles and L. Floridi, ‘A manifesto for the future of the “right to be forgotten” debate’ *Guardian*, 22 July 2014 <<http://www.theguardian.com/technology/2014/jul/22/a-manifesto-for-the-future-of-the-right-to-be-forgotten-debate>>; Koops, *op. cit.*, n 53, p. 250, on ‘clean slate’ social norms.

⁶³ On ‘digital collages’, see Mayer-Schönberger, *op. cit.*, n 28, p. 124.

⁶⁴ See J. van Hoboken, *Search Engine Freedom* (2012).

than any information that is self-published, making so-called ‘online reputation management’ a daunting if not impossible task for individual data subjects.⁶⁵

Restoring, to some degree, the individual’s ability to engage in information games is what we mean when we say that she has interests in being forgotten by others. We will explore what this might mean in practice later in the paper but for now we turn to consider the other aspect of the ‘right to be forgotten’.

(b) The interest in forgetting

The first aspect of the ‘right to be forgotten’, being forgotten by others, gives expression to a control-based understanding of privacy while the second, which we now examine, emphasises dignity. Of course there is a significant conceptual overlap between the first and second aspects as, in Kantian terms, autonomy is the ‘ground for the dignity of human nature’.⁶⁶ But the second aspect speaks more to the traditional dignitarian account as espoused by privacy scholars.⁶⁷ As Mayer-Schönberger has put it, the capacity to forget is an essential part of what makes us human. Being constantly confronted with one’s past is potentially degrading and thus can undermine human dignity.⁶⁸

That our capacity to forget is a necessary component of human agency is an old idea. Nietzsche, for instance, draws our attention to the value of living ‘unhistorically’. For him, forgetting is important because it ensures happiness, however brief the moment.⁶⁹ He warns that if we cannot forget, the past risks becoming ‘the gravedigger of the present.’⁷⁰ In the same way, Kundera attempts to contemplate the sheer horror of an existence in which one is unable to forget. Such a person, he writes, ‘would be nothing like human beings: neither his loves nor his friendships nor his angers nor his capacity to forgive or avenge would resemble ours.’⁷¹ This is because forgetting is ‘part of the essence of man’.⁷²

Though the importance of forgetting for human agency is an old idea, it is more relevant now than ever before. We talk of information technology being pervasive or ubiquitous.⁷³ Indeed, for most in the developed world, online connectivity is no longer a novelty because we are constantly connected. Where there is excessive remembering the past may become overbearing. Old emails, our browsing history and old correspondence on social networking websites are accessible in an instant. We can use the internet to churn up old memories but because they come all at once they threaten to overwhelm and disorient us.⁷⁴ Because forgetting

⁶⁵ For an account of reputation management in practice, see T. Dowling, ‘Search me: online reputation management’ *Guardian*, 24 May 2014 <<http://www.theguardian.com/technology/2013/may/24/search-me-online-reputation-management>>.

⁶⁶ I. Kant, *Groundwork of the Metaphysics of Morals* (ed. M. Gregor, 2011) 43.

⁶⁷ See, for example, Bloustein, op. cit., n 50, p. 1003.

⁶⁸ See, similarly, O.J. Gstrein, ‘The cascade of decaying information: putting the “right to be forgotten” in perspective’ (2015) 21 *Computer and Telecommunications Law Rev.* 40, at 43-44.

⁶⁹ F. Nietzsche, ‘On the Uses and Disadvantages of History for Life’ in *Untimely Meditations*, ed. D. Breazeale (1997) 59-63.

⁷⁰ id., p. 62.

⁷¹ M. Kundera, *Ignorance* (L Asher (tr), 2002) 123.

⁷² id.

⁷³ The idea of ubiquitous computing is not new. Those who have embraced this idea advocate embedding computers into our everyday activities and the objects that we use. As well as placing emphasis on the ‘invisibility’ of technology so that it remains ‘mundane and routine’, they seek to ensure that the technology is ‘smart’ so that it ‘adds value’. See M. Dodge and R. Kitchin ‘Outlines of a World coming into Existence: Pervasive Computing and the Ethics of Forgetting’ (2007) 34 *Environment and Planning B: Planning and Design* 431, at 431.

⁷⁴ Mayer-Schönberger, op. cit., n 28, p. 123.

is necessary for human agency, excessive remembering obstructs human flourishing.⁷⁵ It represents the Nietzschean nightmare of the past becoming the grave-digger of the present, a past from which we are unable to escape.

3. The 'Right to be Forgotten' and the Public Good of Universal Accessibility of Information

The first reason why the 'right to be forgotten' is helpful as a metaphor is because we reveal contemporary privacy-related challenges once we contrast the 'right' with the metaphor of digital technology's 'perfect memory'. At the same time, we have argued that the idea of the 'right to be forgotten' is rooted in the older and more familiar control-based and dignitarian accounts of privacy. In this sense, though *Google Spain* and other recent cases⁷⁶ represent another step in society's ongoing reformulation of what privacy means, this reformulation is not as radical as it first appears.

We now turn to consider the second reason why the metaphor of a 'right to be forgotten' is helpful. Because the terminology is instinctively contentious, it draws our attention to the potential implications of data erasure for the freedom to receive information and freedom of expression, rights integral to every democratic society. In this light, it is worth quoting a passage from the Advocate General's opinion in *Google Spain*:

'In fact, universal accessibility of information on the internet relies on internet search engines, because finding relevant information without them would be too complicated and difficult, and would produce limited results. As the referring court rightly observes, acquiring information about announcements on the forced sale of the data subject's property would previously have required a visit to the archives of the newspaper. Now this information can be acquired by typing his name into an internet search engine and this makes the dissemination of such data considerably more efficient, and at the same time, more disturbing for the data subject.'⁷⁷

Once we accept universal accessibility of information as an important public good it is easy to see how the AG arrived at these conclusions. But this begs the immediate question as to how we reconcile the public good of universal accessibility of information with interests in forgetting/being forgotten.

This question is an especially important one for our argument because up to now we have focussed on the interests of the individual in forgetting/being forgotten. But what is ultimately determined to be an appropriate use of information does not turn solely on the wishes of the individual but is also informed by social norms generally. It is against this backdrop that we now turn to consider Nissenbaum's theory of 'contextual integrity', which sheds light on the question of reconciling the public good of universal accessibility of information with interests in forgetting/being forgotten.

NISSENBAUM'S THEORY OF CONTEXTUAL INTEGRITY

1. Informational Norms and Contextual Integrity

Nissenbaum stresses the sheer variety and complexity of our expectations about the flow of information. These expectations are 'systematically related to characteristics of the background social situation.'⁷⁸ In other words, social interaction is complex – in order to understand the dynamic of the interaction we must always take into account the particular

⁷⁵ *id.*, p. 125.

⁷⁶ C-293/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238; *Vidal Hall and Ors v Google* [2014] EWHC 13 (QB).

⁷⁷ AG Opinion in *Google Spain*, *op. cit.*, n 8, para 45.

⁷⁸ Nissenbaum, *op. cit.*, n 37, p. 129.

context of the interaction. Understood in this way, we interact within a variety of ‘structured social settings’ that have developed over time. Not only do these ‘social spheres’ have different origins, they are also subject to a range of ‘contingencies of purpose, place, culture, historical accident and more.’⁷⁹

Nissenbaum builds her theory of contextual integrity in a framework of ‘informational norms’. Contextual integrity is ‘preserved when informational norms are respected and violated when informational norms are breached.’⁸⁰ These informational norms have evolved over time. They ‘have been finely calibrated to support goals, purposes, and values of social life and kinship, such as trust, accommodation, unconditional regard, and loyalty.’⁸¹ New norms emerge and existing norms are reshaped, but there is always a ‘tension’ between our ‘entrenched social structures and practices’ and the ‘forward-pulling forces of technology.’⁸²

What is appropriate or inappropriate use of personal information depends on existing informational norms. These norms are both backward-looking and forward-looking as Nissenbaum recognises. They are *backward-looking* in the sense that they find their origins in the pre-digital age. Allowing space for forgetting and/or to be forgotten by others has been a key feature of our social structures and practices that have evolved over time. As Mayer-Schönberger reminds us:

‘For centuries, moving from one community to another permitted people to restart their lives with a clean slate, as information about them stayed local. Crossing the Atlantic from Europe to the newly founded United States...let people start from scratch, not just in economic terms, but more importantly in terms of knowledge others had of them. Even moving from one neighbourhood to another in a large city might achieve a similar result. In a sense, such moves were akin to declaring information bankruptcy; one could restart again in control of one’s personal information.’⁸³

The idea of a fresh start in this sense forms a profoundly important part of our cultural memory. Indeed, the idea of making a break with the past is so engrained that, as Halavais points out, it has become ‘almost ritualized’.⁸⁴ So we talk about ‘new year’s resolutions’, ‘starting out on a new career path’, or using the transition from secondary school to university as an opportunity to ‘reinvent oneself’.⁸⁵

Yet, at the same time, our informational norms are *forward-looking*, ready to be shaped by new technological developments. Nissenbaum thinks that people will learn to adapt but ‘these adjustments will not be radical and they will be tempered by explicit and implicit respect’ for the informational norms already entrenched in our social structures and practices.⁸⁶ Thus, we have reason to dispute Mark Zuckerberg’s remarks that privacy ‘is no longer a social norm’.⁸⁷

2. Ensuring an Appropriate Flow of Information

⁷⁹ id., p. 130.

⁸⁰ id., p. 140.

⁸¹ id., p. 229.

⁸² id..

⁸³ Mayer-Schönberger, op. cit., n 28, p. 99.

⁸⁴ A. Halavais, *Search Engine Society* (2009) 11, 145.

⁸⁵ Halavais, id.; see also Zittrain: ‘Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a “fresh start” as an adult, we ought to consider how to implement the idea of a second or third chance into our digital space.’ (J. Zittrain, *The Future of the Internet, and How to Stop It* (2008) 228-229.)

⁸⁶ Nissenbaum, op. cit., n 37, p. 229.

⁸⁷ B. Johnson, ‘Privacy no longer a social norm, says Facebook founder’ *Guardian*, 11 January 2010, <<http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>>.

For Nissenbaum, the battle for privacy is not a battle about being able to erase information at will from the internet. Rather she argues that ‘the right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information.’⁸⁸ What individuals find most disturbing is when there is a ‘clash of contexts’ resulting in an inappropriate flow of information.⁸⁹ These are cases where people ‘have understood themselves to be operating in one context and governed by the norms of that context, only to find that others have taken them to be operating in a different one.’⁹⁰ This might take place where other actors ‘divert’ information flows in an ‘unexpected’ way and this diversion thus breaches informational norms. This is an important point because, as we have already mentioned, traditional distinctions between the public and private spheres have become blurred in the online context. Understood in this way, older informational norms have been reformulated and new norms have emerged. So, by means of illustration, a clash of contexts emerges when an employer obtains via Facebook information about an employee’s socialising habits where these activities have no impact on the employee carrying out his duties.⁹¹

Understood in this way, Nissenbaum’s idea of a ‘clash of contexts’ is not unlike Goffman’s thoughts about ‘audience segregation.’ An integral part of the ‘information game’ is the individual’s ability to display different ‘fronts’ in different contexts. But what amounts to an appropriate or inappropriate flow of information should not be left entirely to the individual to decide. This is because some of our informational norms stem from deeply engrained convictions in society about the ‘public interest’ or the ‘common good’. Mr. Costeja’s complaint in *Google Spain* is a neat illustration of this point. Here information about a real-estate auction of his property, prompted by Mr. Costeja’s social security debts, was legitimately reported by the Spanish newspaper. It was legitimate because the information was relevant news at the time it was originally reported, in the public interest and the newspaper clearly had both a duty and a right to publish it. Within the framework of informational norms existing in a modern democracy, this surely amounts to an appropriate flow of information and thus the principle of contextual integrity is not offended. In some cases, then, the individual may wish to engage in ‘audience segregation’ but the informational norm of the public interest trumps the individual’s wishes. However, in the *Google Spain* case, a ‘clash of contexts’ emerged (and the principle of contextual integrity was thus offended) once a link to the newspaper report became one of the first results to come up about Mr. Costeja in a Google search of his name years later. There was a clash of contexts because, despite the passage of time, Mr. Costeja’s very identity was being shaped by Google searches and this process was to continue indefinitely. Mr. Costeja’s capacity to engage in information games was thus greatly reduced.

If we accept the need for contextual integrity, then, it cannot follow that all information should be made easily and instantaneously available. Where there is an appropriate flow of information (according to existing informational norms, including those stemming from the public interest), there are good reasons to make such information generally available. But where this information flow is inappropriate, there are sound arguments for requiring some

⁸⁸ Nissenbaum, op. cit., n 37, p. 127. For a similar argument see the account by de Andrade (op. cit., n 52) of ‘de-contextualised information’, and R.J. Peltz-Steele, ‘The “Right to be forgotten” online is really a right to be forgiven’ *Washington Post*, 21 November 2014 < https://www.washingtonpost.com/opinions/the-right-to-be-forgotten-online-is-really-a-right-to-be-forgiven/2014/11/21/2801845c-669a-11e4-9fdc-d43b053ecb4d_story.html >.

⁸⁹ Nissenbaum, id., p. 225.

⁹⁰ id.

⁹¹ See, for instance, CareerBuilder, ‘Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise, According to New CareerBuilder Survey’ *CareerBuilder*, 26 June 2014 <<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2f26%2f2014&id=pr829&ed=12%2f31%2f2014>>.

intent on the part of the researcher to find the information. Sometimes, then, contextual integrity demands that *intent* is required to obtain certain types of information. Understood in this way, it should be more difficult to obtain the type of information that would have been buried in the archives in the pre-internet era.⁹² Again, this does not mean that this information should be impossible to access. For all sorts of reasons, historians and journalists, for example, may need to access such information in the future. Moreover, this is not an argument to return to the physical archives of the past. Rather, this argument simply states that if we are to allow sufficient space for forgetting in the digital era then some information should not become instantly available by putting a person's name into a search engine. In the case of Mr. Costeja, contextual integrity could have been preserved had the information about his past social security debts been available in a section of the website of the newspaper but the link to this information was not instantaneously associated with a search for *only* his name, without any qualifiers, on a search engine. This was what the Spanish tribunal had recommended and what the ECJ decision amounts to in effect.

No doubt there will be those who will remain uneasy about such an argument for the reasons we outline in the opening paragraph of this paper. But we would attempt to reassure such readers by emphasising that this argument is not one that seeks to have information erased from the internet, in the sense of outright data deletion. Rather, the argument is that sometimes it better to obtain 'limited' or, as we will argue, 'reordered' results from a search engine as long as this preserves contextual integrity. In short, it is an argument that recognises the special status of search engines in the digital age.

The decision in *Google Spain* thus does something that is in our view paramount: by giving expression to interests in forgetting/being forgotten, it forces us to reconsider our understanding of privacy and its interaction with the freedom to access information in ways that are valuable for the digital age. We have argued that a 'right to be forgotten', in the sense elaborated in section 3 above, has the potential to be a useful metaphor in conceptualising contextual integrity on the internet. However, though its development can be defended in principle, any 'right' seeking to achieve contextual integrity must be delineated and implemented in an appropriate way. Before we conclude, we will examine some of the shortcomings of the Court's judgment and propose how, in practice, the principles that underlie a 'right to be forgotten' can be given effect through functional, procedural remedies.

GOOGLE SPAIN AND CONTEXTUAL INTEGRITY

1. Shortcomings of the Judgment

While most commentary acknowledges that *Google Spain* established a 'right to delist' certain internet search results,⁹³ rather than a 'right to be forgotten', criticism of the Court's findings has all the same been pervasive since it issued its judgment in May 2014. Reasons for academic critique range from principled opposition to any form of 'censorship'⁹⁴ to more general questions as to whether it is appropriate to charge a private party, with clear commercial

⁹² On a Lakoff and Johnson analysis, the metaphorical use of the verb 'to bury' in the phrase 'to bury something in the archives' tells us much about our shared understanding of what should happen to information that becomes out of date. For the authors, '[t]he most fundamental values in a culture will be coherent with the metaphorical structure of the most fundamental concepts in the culture.' See Lakoff and Johnson, op. cit., n 32, p.22.

⁹³ See The Advisory Council to Google on the Right to be Forgotten, *Final Report* (6 February 2015) <<https://www.google.com/advisorycouncil/>> 4.

⁹⁴ See J. Zittrain, 'Don't Force Google to "Forget"' *New York Times*, 14 May 2014 <http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0>; and J. Rosen, 'The Right to be Forgotten' (2012) 64 *Stanford Law Rev. Online* 88.

interests, with balancing very sensitive and competing human rights when such balancing is a struggle even for courts.⁹⁵ Legal scholars have been particularly critical of the judgment's own weighing of the competing rights, with James observing that the decision 'leans firmly (almost to the point of falling over) on the side of the right of privacy...'.⁹⁶ Frantziou adds to this a critical comparison of *Google Spain* with the jurisprudence of the European Court of Human Rights. In *Węgrzynowski*, the ECtHR found that 'particularly strong reasons must be provided for any measure limiting access to information which the public has a right to receive'.⁹⁷ Frantziou notes that any assessment of the impact of a 'right to delist' on the competing rights to freedom of expression and information is 'starkly missing' from *Google Spain*.⁹⁸ Furthermore, concern has also been expressed about the fact that Google's process of handling requests is couched in secrecy.⁹⁹ A July 2015 data leak of Google's responses to requests suggests that the bulk of the requests relate to clearly 'private' information, but sheds no particular light on Google's actual processes of handling requests.¹⁰⁰

Of most interest given the focus of this article, however, is the criticism that has been levelled against the substantive 'delisting' criteria that the ECJ unearthed from the Data Protection Directive. Commentators have flagged up that hinging a 'delisting' request on the 'relevance' of data is very problematic, as relevance is contextual: information about a fourteen year old child today may become information about the UK prime minister in 40 years' time, and an old bankruptcy notice such as Mr. Costeja's may once again become 'relevant' if he encounters further financial difficulty.¹⁰¹ A search engine like Google making 'relevance' determinations is particularly controversial, as search engines organise information in light of their own business interests.¹⁰² A search engine that simply produced a value-neutral list of results without ordering them would be unusable; its results would simply not be 'relevant' to most of its users, at which point its profits (rooted in the amount of usage it attracts) would dwindle.¹⁰³ Google's search algorithm consequently tracks popularity of pages as a specific measure of 'relevance'. There is no guaranteeing that private information will not be popular, and consequently of public interest, in Google's view; Google therefore must be told explicitly how concepts such as 'relevance' and 'preponderant interest' are to be interpreted.

The EU's Article 29 Working Party, an EU-level advisory body composed of national DPA representatives, has issued guidance to search engines on when to 'delist'. However, it is significantly hampered in its attempts to provide detailed guidance by the sparsity of the Court's reasoning. In *Google Spain*, terms such as 'relevance', 'preponderant interest' and

⁹⁵ See Lynskey, op. cit., n 6, p. 532; Lindsay, op. cit., n 13, pp. 178-179; European Union Committee, *EU Data Protection law: a 'right to be forgotten'?* (HL 2014-2015, 40) para 36.

⁹⁶ S. James, 'The Right to Privacy catches up with search engines: the unforgettable decision in *Google Spain v AEPD*' (2014) 20 *Computer and Telecommunications Law Rev.* 130, at 132.

⁹⁷ *Węgrzynowski and Smolczewski v Poland* App no 33846/07 (ECHR, 16 July 2013) para 57; see also *Timpul Info-Magazin and Anghel v Moldova* App no 42864/05 (ECHR, 27 November 2007) para 31.

⁹⁸ E. Frantziou, 'Further Developments in the Right to be Forgotten' (2014) 14 *Human Rights Law Rev.* 761, at 772; see also Lynskey, op. cit., n 6, p. 530.

⁹⁹ See J. Kiss, 'Dear Google: open letter from 80 academics on 'right to be forgotten'' *Guardian*, 14 May 2015 <<http://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten>>; J. Powles, 'Google's data leak reveals flaws in making it judge and jury over our rights' *Guardian*, 14 July 2015 <<http://www.theguardian.com/technology/2015/jul/14/googles-data-leak-right-to-be-forgotten>>.

¹⁰⁰ S. Tippman and J. Powles, 'Google accidentally reveals data on 'right to be forgotten' requests' *Guardian*, 14 July 2015 <<http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests>>.

¹⁰¹ European Union Committee, *EU Data Protection Law: a "Right to be Forgotten"? : Evidence* (July 2014) <<http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/righttobeforgotten/right-to-be-forgotten-evidence.pdf>> 20, quoting L Floridi.

¹⁰² See, inter alia, Lynskey, op. cit., n 6, p. 532.

¹⁰³ Halavais, op. cit., n 84, p. 103.

‘public life’ are presented as if they either fully apply or do not apply. Given that starting point, there is limited scope for the Working Party’s guidance on the judgment to take into account context-dependent gradations of ‘relevance’ and ‘interest’. It is clear that the guidance attempts to consider informational context in a more explicit manner than the judgment did: it embraces that, for instance, information about children is more likely to require ‘delisting’ than identical information about adults would be.¹⁰⁴ However, the guidance generally merely alludes to contextual considerations that search engines may wish to consider—such as ‘age of the information’—without setting down benchmarks that search engine decision-making can be measured against. This will not greatly help search engines in processing ‘delisting’ requests where the indexed information may be *slightly* relevant, or *of some* public interest. The guidance, in short, is too general; but that generality is an inevitable consequence of *Google Spain*, which established a very broad remedy.

The ECJ in *Google Spain*, then, has set out too little in its judgment that will safeguard the contextually relevant balancing of the rights to information and the right to privacy. While we stand by the idea that not all information on the internet needs to remain instantly accessible indefinitely, *Google Spain* establishes a procedural remedy that does not necessarily ensure that information flows *appropriately* in the way that contextual integrity demands.

2. In Defence of Google Spain

We would argue, however, that criticism of the judgment must itself be contextualized. It must be remembered that in many ways, *Google Spain* is a blunt-force application of a Directive from 1995 to the 2014 internet. As the AG astutely notes, it was drafted at a time when it was not yet conceivable that the internet would become a ‘comprehensive global stock of information which is universally accessible and searchable.’¹⁰⁵ It is not equipped to cope with the effects that search engines have had on the rights at stake in the *Google Spain* case: information is more readily available and data subject privacy has become more complicated to guarantee than was ever deemed possible in 1995. The judgment thus works with outdated concepts that suggest that personal data is available online in a limited manner that can be easily controlled by a single data controller—an idea that seems a little naïve in the Google age.¹⁰⁶

What most commentators have not stressed enough in our view is that the alternative to finding a ‘right to delist’ would have been to conclude that under the current interplay between the Data Protection Directive and the Charter of Fundamental Rights, internet users in the EU simply cannot exercise *any* degree of control over the picture that Google paints of them. They may have had data protection rights in a more general sense, but they would have no particular power to act against search engines, who previously believed themselves to only be information ‘intermediaries’, not generally subject to EU data protection law.¹⁰⁷

This would have been a very problematic conclusion, fixed on an interpretation of what search engines do that is as outdated as the Directive. As stressed above, Google does not simply ‘list’; it constructs online identities of data subjects without their input. When information about a data subject is available online, Google will ‘crawl’ it, index it, and then rank it according to its mysterious algorithms. Data ‘ranking’ has particular identity-

¹⁰⁴ Article 29 Data Protection Working Party, ‘Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12’ (26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> 15.

¹⁰⁵ AG Opinion in *Google Spain*, op. cit., n 8, para 27.

¹⁰⁶ See also Lindsay, op. cit., n 13, p. 160.

¹⁰⁷ *Google Spain*, op. cit., n 1, para 22.

constructing implications, which *Google Spain* addresses for the first time.¹⁰⁸ Mr. Costeja was unable to play an effective ‘information game’; his identity was set in stone by Google’s search ranking of an old newspaper clipping that had his name in it. Though that information was clearly ‘relevant’ and of public interest in 1998, and thus legitimately made available in one context, it was years later being reproduced by Google without the same *prima facie* ‘relevance’ or public interest. The end result was that Mr. Costeja could not engage in ‘audience segregation’ because his audience already possessed information about him, despite the *prima facie* irrelevance of that information to the public. In this way, the presence of the link in the search engine results offended contextual integrity.

In short, without the ability to somehow address the identity-constructing that search results engage in, identity-related aspects of the right to privacy were definitely not adequately protected by EU law before *Google Spain*. The judgment thus engages with outdated law in a forward-looking way, making clear that the modern internet does not have to mean a degradation of dignity.¹⁰⁹ Nonetheless, the judgment—restrained by both the legal terminology of the pre-Google era and a very specific referred question—is premised on an oversimplification of the difficult relationship between the human rights at stake in the Google era. In exclusively considering the potential removal of a particular search result, the judgment paints a picture of the public’s relationship to Google as being a very fixed, binary one: either Google respects our privacy and so it ‘delists’, or it does not. The reality of Google’s functioning is more complicated, in a way that the judgment simply cannot grapple with given the limitations of the Data Protection Directive. Google does not simply ‘forget’ or ‘remember’, nor does it simply produce a plain catalogue of all available information when a search term is entered: its ‘ranking’ process is not neutral, and does not necessarily pay heed to the context surrounding information that it indexes.¹¹⁰ As Pasquale has said, ‘Search results pages are a messy ground of contestation, influenced by search-engine optimizers, engineers within Google, paid ads, human reviewers of proposed algorithm changes, and many other factors.’¹¹¹ What this means is that data subjects cannot simply assume that the flow of information pertaining to them respects contextual integrity once it is indexed and presented as a search result by Google.

3. Contextualizing the Google Spain Right

The ultimate battle fought by Mr. Costeja concerned the ease with which information about him could be accessed, on a search of *only* his name, through Google. The Court’s solution was to make the information harder to find by simply not having it indexed. While the media frenzy surrounding *Google Spain* has meant that Mr. Costeja did not personally benefit from the established remedy, such a remedy will serve the purpose of future individuals in similar situations.¹¹² However, Mr. Costeja’s is an extreme example of how Google shapes identity. In many more instances, while the information presented by Google may not result in

¹⁰⁸ See European Union Committee, op. cit., n 101, p. 15, quoting C Scott.

¹⁰⁹ This is broadly in line with the ECtHR’s interpretation of the right to privacy, which encompasses ‘the right to establish details of their identity as individual human beings’; see *Goodwin v United Kingdom* App no 28957/95 (ECHR 11 July 2002) para 90; *Pretty v United Kingdom* App no 2346/02 (ECHR 29 April 2002) para 62; *Mikulić v. Croatia* App no 53176/99 (ECHR 7 February 2002) para 53.

¹¹⁰ Halavais, op. cit., n 84, pp. 103-105.

¹¹¹ As quoted in J. Sadowski, ‘Lessons from the “right to be forgotten”’ *The Hill*, 1 June 2014 <<http://thehill.com/blogs/pundits-blog/technology/207841-lessons-from-the-right-to-be-forgotten>>.

¹¹² Commentators have correctly observed that Mr. Costeja’s bankruptcy is, as a result of *Google Spain*, less ‘forgotten’ than it has ever been – but his is likely one of very few high-profile cases to surface now that a remedy to ‘delist’ is accessible directly from search engines.

constant negative personal repercussions, it will nonetheless be perceived by data subjects as more or less relevant to them at differing points in time.

Our concern about *Google Spain* is that, in introducing ‘delisting’ as the only remedy to data ‘relevancy’ problems, the case establishes a one-size-fits-all approach to highly variable situations. It is not unlike holding that when earlier work experience is no longer relevant to a current job application, it forever disappears from a CV. This fully ignores that there may be context-dependent degrees of ‘irrelevant’, and that these may vary over time. What data subjects have lost with the advent of search engines and web 2.0, and what they ideally would regain, is assurance that the internet presents information about them in a manner that society—rather than Google’s algorithm—finds contextually appropriate. *Google Spain* remedies this situation to an extent, but not necessarily in all situations.

For some data, such as data pertaining to a teenager’s ‘youthful indiscretions’ or any person’s ‘spent’ legal troubles, our societal expectations are in fact those of a clean slate: we socially and legally accept that certain experiences we undergo are consigned to history, and should not be automatically associated with an individual by name for the remainder of their lives.¹¹³ An example of this in UK legislation is the Rehabilitation of Offenders Act 1974. The UK Supreme Court in *T and Anor* in 2014 confirmed, amongst other things, that disclosing two bicycle thefts at age eleven every time the now-adult respondent applied for a position that involved interaction with children was an unnecessary (and thus unjustified) intervention with his private life.¹¹⁴ ‘Delisting’ search results that pertain to this type of information appears to respect contextual integrity, but is not the only possible remedy to clashes of contexts.

Alternative ways of preserving contextual integrity have been proposed both prior to and in the aftermath of the *Google Spain* judgment. Mayer-Schönberger, for instance, has long advocated for the automatic expiration of information, which could be extended to an expiration of search results; this would be one way of mimicking ‘memory’ on the internet.¹¹⁵ However, such an approach preferences privacy over the right to information as a default, if enough time has lapsed. This will not always be contextually appropriate, and is therefore not an improvement to ‘delisting’.

A different solution has been proposed by Powles and Floridi, who have argued for a ‘comment’ function on search results, enabling data subjects to provide context to the information about them.¹¹⁶ As a remedy, this ‘comment’ function would preserve freedom of information to the full extent, while enabling the data subject to play some form of an ‘information game’. However, it fails to achieve what Mr. Costeja actually sought to obtain from Google, and what many others will desire: a decrease in focus on certain bits of information, because their relevance has diminished with time. A comment on Google’s search results from Mr. Costeja, explaining that the newspaper notices in question were no longer relevant, would do little to negate the first impression created by the existence of those notices on the first page of search engine results. The explanation would merely offer a ‘defence’ of sorts – but the argument made by Mr. Costeja, which we believe to be entirely valid, is that he should not be made to ‘defend’ twelve year old behaviour for the rest of his life simply because Google has ranked this information as relevant. A ‘comment’ function remedy would thus preference the right to information over the right to privacy, as the original information would never disappear; again, this may not always be contextually appropriate.

What *Google Spain* has demonstrated a need for is a remedy that acknowledges that the relevance of information varies with the passage of time, and search engine results for plain

¹¹³ Stuart, op. cit., n 10, pp. 509-510; de Andrade, op. cit., n 52, p. 133; Section 3 above.

¹¹⁴ *R (on the application of T and another) (Respondents) v Secretary of State for the Home Department and another (Appellants)* [2014] UKSC 35, para 142 (Lord Reed).

¹¹⁵ Mayer-Schönberger, op. cit., n 28.

¹¹⁶ Powles and Floridi, op. cit., n 62.

name searches of individuals should reflect such variance. Consider, for instance, information that is not necessarily harmful or prejudicial to the data subject, the way that a reminder of a twelve year old bankruptcy would be, but information that is simply of *lesser relevance* to that data subject; information that may not be offensive, but nonetheless would not make the first page of someone's CV or the first hour of conversation with a new acquaintance.¹¹⁷ We would argue that such information should also not appear on the first page of Google's search results for a data subject's name, but does not need to be 'delisted' and thus disassociated with that person's name forever. As Zittrain notes, 'the second page [of search results] ... might as well be in Siberia'.¹¹⁸ If few internet users will look past the first page of results, this suggests that the most 'relevant' information should be on this page, and less 'relevant' information should be less visible. A means of achieving this kind of contextual integrity in search results is, as Stuart has persuasively set out in the US context, enabling data subjects to request a 'reordering' of Google search results produced for their name.¹¹⁹ Introducing a 'reordering' remedy alongside the existing 'delisting' remedy established by *Google Spain* would permit users to indicate what information, on a plain search of their name, is more and less relevant about them at any given point in time, as well as (where information warrants this) requesting for certain information to simply not appear at all anymore.

A 'right to reorder' would not need to result in permanent, static search engine result editing: while a request could trigger a 'downranking' of information, Google's PageRank algorithm could thereafter continue to apply to it, meaning that if a particular piece of online information becomes more 'relevant' with time again (as measured by search popularity, or perhaps cross-referencing in other online sources), it would move back up on the search results pages – in an automated analogy to someone amending their CV in light of the 'essential criteria' in a particular job application.

A potential criticism of a 'reordering' of search results would be a lack of transparency in the actual reordering process; while 'delisting' is a clear process from the perspective of the publisher, 'reordering' requires changes to the Google algorithm that will be as couched in secrecy as the algorithm itself. However, while 'reordering' as a remedy may have less *clear* consequences for publishers and information seekers, it also has less *extreme* consequences for these parties than 'delisting' does. For that reason, we would argue that it balances these competing rights in a generally preferable way even if slightly less transparent.

The role of the Article 29 Working Group would be key in establishing 'reordering' as a remedy: its guidance would need to set out the relationship between the *context* of given information about data subjects, and the extent of *reordering* required of the search engine in light of that context. The flexibility offered by a request to reorder, as well as its non-static application, would ensure a far greater degree of contextual integrity in information flows than the binary of keeping or 'delisting' established by *Google Spain*. Any ensuing Working Group's guidance, drafted as the outcome an EU-wide debate amongst DPAs of societal expectations surrounding data privacy, would be able to explicitly consider gradation of terms such as 'relevance' and 'preponderant interest' in a way that its current guidance cannot, because this additional remedy can represent different *degrees* of 'relevance' and 'preponderant interest' of information. Such guidance would also shed light on the 'reordering' process itself, addressing the transparency concerns highlighted above by establishing benchmarks for Google's 'reordering' choices.

The fact that search engines are likely to announce that they are 'reordering' information, in the same way that Google now notifies users that some results may not show

¹¹⁷ See, for similar considerations, P Korenhof et al., op. cit., n 7, p. 192.

¹¹⁸ J. Zittrain, 'The Ten Things That Define You' *Technology Academics Policy*, 15 May 2014 <<http://www.techpolicy.com/Blog/May-2014/Ten-Things-That-Define-You,-The.aspx>>.

¹¹⁹ Stuart, op. cit., n 10, p. 463.

as a consequence of *Google Spain*, is unlikely to cause significant problems when it comes to preserving the right to privacy. While ‘reordering’ may have a certain novelty factor when it is first announced—and may thus result in users assessing far more search results pages than they ordinarily would—the fact that it is a general notice, applicable to all name searches regardless of whether they are subject to ‘reorder’ or ‘delisting’ requests, suggests that after perhaps a few cursory attempts to see if there are any ‘interesting’ results on later pages, most users would return to ordinary search behaviour. After all, over 95% of EU-based Google searches continue to originate from localised Google search domains for their particular country, meaning users have not switched to using Google.com instead, even though Google suggests that that is where the real interesting search results now live.¹²⁰

Practical objections to a right to ‘reordering’ are likely to be similar to objections to the development of a ‘right to be forgotten’. However, *Google Spain* has already conferred an obligation for Google to engage with any data subject on a case-by-case basis where they believe a search of their name produces inaccurate or out of date information, and it has proved capable of doing so administratively and willing—despite initial protests—to ‘edit’ its search engine results to comply with the law.¹²¹ What we argue for is a more ‘nuanced’ approach to addressing search engine obligations. The EU legislator, by merely codifying a ‘right to erasure’ in the forthcoming General Data Protection Regulation, missed an opportunity to specifically address the increasingly significant role that search engines play in identity formation for most data subjects.¹²² In requiring search engines to process both ‘delisting’ requests and ‘reordering’ requests, we argue that the right to privacy of data subjects will be better protected, and freedom of information will also be better preserved. ‘Delisting’ ideally would occur only when contextual integrity suggests that information has to be fully *disassociated* from an individual’s name; it should function as the exceptional remedy, reflecting that there are only limited types of information that impact on private life where there is a societal expectation of complete ‘erasure’.¹²³ Where this very high standard cannot be met, reordering will nonetheless enable the data subject to play an ‘information game’, restructuring their online identity as it develops and thus preserving their right to privacy in a contextually appropriate manner. Either type of request will require Google to make difficult judgments of when information is ‘relevant’ or what the public interest is, and the Article 29 Working Group and the EU legislator should spend a substantial amount of time considering what conditions should apply for either type of request to be successful.¹²⁴ This will undoubtedly not be a simple task, but unless privacy and the freedom to access information actually cease to be a social norms that we wish to safeguard, it is a necessary step to make data protection rights workable in the future.¹²⁵

CONCLUSIONS

¹²⁰ The Advisory Council, op. cit., n 93, p. 19.

¹²¹ Koops, op. cit., n 25, questioned in July 2014 ‘whether and how’ Google will continue to comply with the judgment (p. 253); however, at the time of writing in January 2016, there are no signs of it having abandoned case-by-case analysis (see Google, ‘European privacy requests for search removals’ <<http://www.google.com/transparencyreport/removals/europeprivacy/>>).

¹²² European Council Presidency, op. cit., n 27, Article 17.

¹²³ One possible means of distinguishing between the two types of request is, as Hörnle has suggested, to rewrite EU data protection legislation so as to make it clear that delisting is a right that is contingent on the information in question being prejudicial to a data subject. (J. Hörnle, ‘Google’s algorithms, search results and relevancy under data protection law – whose data quality?’ (2014) 25 *Entertainment Law Rev.* 209, at 212.)

¹²⁴ See also Hijmans, op. cit., n 13, p. 562.

¹²⁵ As discussed in Section 3, Nissenbaum (op. cit., n 37) argues that our informational norms will not adjust radically; whereas Mayer-Schönberger (op. cit., n 28, pp. 156-157) concedes that they may change radically, but that such achievement will take generations. Either view justifies legislative action beyond the ‘right to erasure’ (‘right to be forgotten’) in Article 17 of the General Data Protection Regulation at the EU level at this time.

The ‘right to be forgotten’ has attracted a significant amount of criticism, much of it stemming from dissatisfaction with the terminology. As Zimmerman forcefully argued some years ago, ‘woolly’ concepts have no place in our laws.¹²⁶ Most of the critics of the ‘right to be forgotten’ would appear to concur.

We have argued, however, that the ‘right’ can be put to good use as a metaphor. This metaphor helps us better understand not just the new and emerging privacy concerns of the digital age but also how these concerns impact on the public good of universal accessibility of information.

Once we pay attention to the dual nature of the ‘right’ we see that fundamental interests in autonomy and dignity are at stake. In particular, while the construction of identity is a social as well as a personal process, we have argued that playing an ‘information game’ in Goffman’s sense is increasingly difficult online but no less necessary. Restoring, to some degree, the ability to engage in information games on the internet is what a proper development of the ‘right’ would accomplish. To borrow Koops’ expression, *Google Spain* ‘provides a glimmer of hope’ for regaining some degree of control over the various information flows that shape our identities.¹²⁷

We have emphasised too that Nissenbaum’s idea of contextual integrity provides us with important insights about the ‘right to be forgotten’ and its relationship with the freedom to access information. Rather than think solely in terms of a binary of remembering and forgetting (that is, either we keep the information or we erase it), we argue that it is better to question instead whether there is an *appropriate* flow of information. Understood in this way, it is not necessarily the case that the best way to ensure contextual integrity in a given case is to erase search engine results. Indeed, we have argued that the erasure tool should be available only in those cases where there is a societal expectation of a ‘clean slate’. Where this high threshold is not met, reordering the information might appropriately balance data subject privacy and freedom of information. Offering two potential remedies rather than one would be no easier to implement than *Google Spain*’s ‘right to delist’ or the General Data Protection Regulation’s ‘right to erasure (“right to be forgotten”)’—but crucially, it would also not be more difficult. At the same time, we would argue that the upshot is that such a solution would be better able to ensure contextual integrity, to safeguard interests in privacy as well as the freedom to access information.

¹²⁶ Zimmerman, op. cit., n 38.

¹²⁷ Koops, op. cit., n. 25, p. 255.